

TJENESTE FOR HERDING AV ENHET

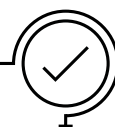
Canons tjeneste for herding av enhet bidrar til å forbedre ytelsen til en utskriftsenhet og gjøre den motstandsdyktig mot sikkerhetsrelaterte problemer. Tjenesten vår forbedrer den innebygde sikkerheten til Canon-enheter ved å bruke en sikker profil for ekstra beskyttelse uten ekstra innsats.



ANBEFAL



KONFIGURER



VALIDER



FORRETNINGSMESSIGE FORDELER:

- Redusert risiko for datatap ved å beskytte data som er lagret på enheter gjennom hele levetiden
- Utvid bestemmelsene om personvern til å omfatte skriverenheter for å opprettholde et sikkert miljø
- Reduser risikoen for printrelaterte sikkerhetsbrudd og unngå faren for mulige bøter og skade på merkevarens omdømme



POTENSIELLE FORRETNINGSMESSIGE TRUSLER

- Enhetene lagrer og behandler konfidensielle data, for eksempel økonomiske rapporter og annen sensitiv informasjon
- Enhetene står i nettverk, noe som kan utsette dem for potensielle angrep
- Enhetene anses ofte ikke som sikkerhetsutfordringer, noe som igjen kan gjøre dem til større mål

TJENESTE FOR HERDING AV ENHET

KONFIGURASJON AV HERDING AV ENHET

En sikker profilkonfigurasjon som er fullstendig testet, og som omfatter anbefalte fremgangsmåter og forventninger for cybersikkerhet fra kjøpere av sikkerhetsløsninger.

Canon tilbyr også en skreddersydd tjeneste som dekker kundespesifikke krav.

FUNKSJON	BESKRIVELSE
Aktiver funksjonen for sikker sletting av data	Data slettes automatisk fra enhetslagringen etter hver jobb når alle sidene er skrevet ut / fakset / skannet / kopiert.
Angi passord for eksternt brukergrensesnitt	Eksternt brukergrensesnitt gir tilgang til enhetsinnstillinger via Internett. Passord gir autorisert tilgang til dette grensesnittet.
Angi passord for System Manager	Gjennom System Manager får du tilgang til enheten med administratorrettigheter. Passordet endres fra fabrikkinnstillingen for ekstra beskyttelse.
Angi passord for Remote Management-verktøyet	Gjennom remote-verktøyet får du ekstern tilgang til enhetens berøringspanel og servicegrensesnitt. Passord gir ekstra sikkerhet.
Aktiver verifisering av systemintegritet ved oppstart	Sikker oppstart er en innebygd funksjon som kontrollerer om det er endringer i BIOS, firmware eller MEAP-programmene når enheten startes.
Skjul jobblogger	Blokker visning av jobblogger som genereres på enheten, siden disse kan omfatte filnavn og brukernavn.
Deaktiver ubrukte protokoller og tjenester	Enkelte aktive protokoller og porter kan øke risikoen for angrep. Derfor deaktiveres slike ubrukte innstillinger. Disse omfatter SMB, FTP og IP-faks.
Begrens bruken av USB	Enheden kan ikke kobles til en PC via USB for å kunne bruke utskrifts- og skannefunksjoner. Skannede dokumenter kan ikke lagres på en USB-minnepinne.
Begrens tilkobling til trådløse nettverk	Enheden kan ikke kobles til bedriftsnettverket via Wi-Fi.
Forby tilgang for gjestebrukere	Uregistrerte brukere kan ikke logge på for å bruke enhetsfunksjoner, inkludert frigi utskriftsjobber som sendes via sikker utskrift fra enhet.
Tving automatisk avlogging	Brukere logges av automatisk hvis ingen operasjoner utføres i løpet av 30 sekunder.
Begrens bruken av svake krypteringsalgoritmer	Tilkobling til systemer som støtter svak kryptering relatert til IPSec, TLS, Kerberos, S/MIME, trådløst LAN og SNMPv3, deaktiveres.

KONTAKT

Kontakt ditt lokale Canon-kontor for å få mer informasjon.

Canon Inc.
canon.com

Canon Norge
canon.no

Norwegian edition
© Canon Europa N.V. 2023

Canon Norge AS
Hallagerbakken 110
Postboks 33 Holmlia
1201 OSLO
Tlf. +47 2262 9200
canon.no